Forderungspapier

NIS-2 Gesetz

25. November 2024

Ausgangslage

Die Vorteile der NIS-2-Richtlinie können nur durch eine durchdachte und zielgerichtete Umsetzung voll ausgeschöpft werden[1]. Der vom Nationalrat am 03.07.2024 abgelehnte Entwurf[2] wurde diesen Ansprüchen nicht gerecht, wie die zahlreichen, teils sehr umfangreichen Stellungnahmen[3] deutlich machten. Unser Ziel ist es, mit der Umsetzung von NIS-2 eine solide Basis für ein hohes Cybersicherheitsniveau zu schaffen, die klare Verantwortlichkeiten, Transparenz und einen offenen, zukunftsorientierten Austausch zwischen allen relevanten Akteuren fördert, ohne dabei unverhältnismäßige Eingriffe in die Grundrechte und Grundfreiheiten vorzunehmen. Um dies zu erreichen, sind mehrere Aspekte von zentraler Bedeutung:

1. Einrichtung der Cybersicherheitsbehörde als unabhängige Stelle

Im abgelehnten Entwurf war vorgesehen, den Bundesminister für Inneres als Cybersicherheitsbehörde einzurichten. Dies birgt jedoch Zielkonflikte, da die Prioritäten des Innenministeriums oft bei Strafverfolgung und Gefahrenabwehr liegen, was die klare und ausnahmslose Ausrichtung auf die IT-Sicherheit erschwert.

Ein weiteres Problem ist die Personalausstattung. Laut Rechnungshofbericht[4] waren weder das Bundeskanzleramt noch das Innenministerium in der Lage, die vorgesehenen Planstellen zu besetzen, da qualifizierte IT-Fachkräfte in der Privatwirtschaft deutlich besser entlohnt werden. Eine flexiblere Struktur, wie etwa eine gemeinnützige GmbH, könnte mit attraktiveren Arbeitsbedingungen Abhilfe schaffen.

Zudem ist die Einbindung von Wissenschaft und Zivilgesellschaft unerlässlich. Politische Forderungen, die nicht dem Stand der Technik oder den Grundrechten entsprechen, wie ein „Verschlüsselungsverbot", erschweren den Austausch und könnten Österreich in der Cybersicherheit zurückwerfen.

Wir plädieren daher für eine unabhängige Stelle, die sich langfristig und unbeeinflusst von kurzfristigen politischen Debatten allein der anspruchsvollen Aufgabe widmen kann, die Cybersicherheit nachhaltig zu stärken.

1 https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_Statement_NIS_2.pdf
2 https://www.parlament.gv.at/gegenstand/XXVII/ME/326
3 https://www.parlament.gv.at/gegenstand/XXVII/ME/326?selectedStage=101
4 https://www.rechnungshof.gv.at/rh/home/home/2022-13_Koordination_Cyber-Sicherheit.pdf , Seite 93

2. Angemessene Kompetenzen und Datenverarbeitungsmöglichkeiten für die Cybersicherheitsbehörde

Wir unterstützen eine Behörde, die über die notwendigen Kompetenzen verfügt, um effektiv auf Sicherheitsvorfälle zu reagieren. Gleichzeitig müssen die gesetzlichen Bestimmungen so gestaltet sein, dass die Behörde über keine überschießenden Befugnisse verfügt und grund- und datenschutzrechtliche Erwägungen prioritär in diverse Erwägungen zur Behebung von Sicherheitsvorfällen einfließen. Die Datenerhebung und -verarbeitung sollte klar geregelt und auf das Nötigste begrenzt sein, um Missbrauch vorzubeugen und den Datenschutz zu gewährleisten. Eine Balance zwischen notwendiger Handlungsfähigkeit und Schutz und Gewährleistung von Grundrechten ist unerlässlich.

3. Einrichtung eines Technischen-Wissenschaftlichen Beirates für Cybersicherheit

Eine erhöhte IT-Sicherheit in Österreich kann nur durch die enge Zusammenarbeit aller relevanten Akteure gewährleistet werden. Daher ist ein offener Austausch zwischen Staat, Wirtschaft, Zivilgesellschaft und Forschung unerlässlich. Italien zeigt mit seinem Technisch-Wissenschaftlichen Beirat (Comitato tecnico-scientifico[5]), der die nationale Cybersicherheitsbehörde berät, wie dies gelingen kann.

Dieses Gremium vereint Expert:innen aus IT-Sicherheit, Wirtschaft, Verwaltung und Wissenschaft, um langfristige Entwicklungen frühzeitig zu erkennen und zu berücksichtigen. Ein ähnliches Modell in Österreich – erweitert um zivilgesellschaftliche Aktuere, um tatsächlich eine umfassende Beteiligung sämtlicher relevanter Gesellschaftsbereiche zu gewährleisten - könnte eine enge Zusammenarbeit fördern und transparente Ergebnisse liefern, die als Grundlage für politische Entscheidungen dienen.

Ein solcher Beirat schafft eine fundierte Basis, um innovative Ansätze mit gesellschaftlichen und wirtschaftlichen Bedürfnissen in Einklang zu bringen und die Cybersicherheit nachhaltig zu stärken.

4. Echter Schutz der verantwortungsvollen Offenlegung von Schwachstellen

Die aktuelle Rechtslage in Österreich ermöglicht die strafrechtliche Verfolgung verantwortungsvoller Sicherheitsforscher nach §118a StGB, was Unsicherheit schafft und die Offenlegung von Schwachstellen hemmt. Führende EU-Staaten fördern hingegen bewusst diese Offenlegung, und auch die Europäische Agentur für Cybersicherheit (ENISA) plädiert klar für die Abschaffung solcher Regelungen[6].

Der bisherige Gesetzesentwurf entspricht in diesem Aspekt zwar den Vorgaben der NIS-2-Richtlinie, verfehlt jedoch das Ziel, die koordinierte Offenlegung von Schwachstellen zu erleichtern. Erwägungsgrund 60 der Richtlinie fordert nicht nur anonyme Meldungen, sondern auch klare Regelungen für straf- und zivilrechtliche Fragen. Derartiges sucht mach derzeit in Österreich vergebens. Wir fordern daher einen rechtlichen Rahmen, der Sicherheitsforscher:innen schützt und rechtliche Risiken klar adressiert. Ein solcher ist entscheidend, um Vertrauen zu schaffen und die Zusammenarbeit zwischen Forscher:innen, Unternehmen und Behörden zu stärken.

5 https://www.acn.gov.it/portale/en/comitato-tecnico-scientifico

6 Vgl Seite 74 Report „Coordinated Vulnerability Disclosure Policies in the EU", ENISA, April 2022, Link: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu

5. Einführung von Disclsoure Policies und Bug Bounty Programmen für die öffentliche Verwaltung.

Der kostengünstigste Weg die Sicherheit von staatlichen IT-Systemen zu erhöhen, ist die Einführung einer Disclosure Policy und eines Bug Bounty Programs mit symbolischen Beträgen. Dadurch wird ein geordneter Weg für das Melden von Sicherheitslücken geschaffen und Rechtssicherheit geschaffen. Langfristig können damit die Kosten für Sicherheitsüberprüfungen (Audits) durch externe Dienstleister oder hohe Kosten im Falle von Sicherheitsvorfällen (bspw Hack des Land Kärnten) eingespart werden. Das BMK hat dies erst vor kurzem vorgezeigt[7].

Schlussfolgerung

Mit diesen Forderungen möchten wir zur Schaffung einer Grundlage für eine nachhaltige und ausgewogene gesetzliche Grundlage beitragen. Cybersicherheit muss nicht nur auf technischer, sondern auch auf struktureller und rechtlicher Ebene gestärkt werden, um langfristig widerstandsfähig zu bleiben. Die vorgeschlagenen Maßnahmen zielen darauf ab, eine sichere und transparente digitale Infrastruktur zu fördern, die das Vertrauen der Bürger:innen stärkt und die Innovationsfähigkeit der Wirtschaft unterstützt.

7 https://www.ots.at/presseaussendung/OTS_20240906_OTS0104/bmk-it-sicherheitsluecke-durch-hinweis-eines-engagierten-it-kenners-verhindert-keine-daten-von-buergerinnen-betroffen und https://epicenter.works/content/datenleck-beim-klimabonus-richtige-lehren-fuer-die-zukunft